DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION

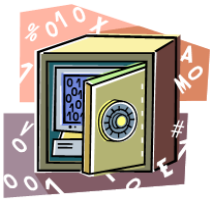
August 2008 Issue

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government

DTI eSecurity News - Using Encryption to Protect Data

What is encryption?



Encryption is the process of altering information to make it unreadable to unauthorized parties. An encrypted message looks like a random series of letters, numbers, and characters.

In order to transform the encrypted message into readable text, the correct decryption key (code) is required. Encryption is particularly important when sending non-public and confidential information such as credit-card numbers, social security numbers, IDs, and passwords.

Types of encryption for Cyber Security

Hardware-based

Hardware-based encryption is built into a piece of hardware. There are pre-encrypted hard drives that are currently on the market, and all data stored in them is automatically encrypted. Pre-encrypted USB drives, for example, are available for purchase.

Software-based

Software-based encryption refers to an encryption program installed on a computer, or a server, that encrypts either some, or all, of the data on the system.

Protecting Your Information

With the increasing use of computers and the need to protect the information on those computers, the use of encryption has expanded.

Laptop protection – Protecting data on laptops can be done by encrypting specific directories and files or by encrypting the entire hard drive (full disk encryption). Minimally, file level encryption should be implemented; full disk encryption is a best practice.

Removable Media – CDs, DVDs, and USB flash drives can hold large amounts of data. They also are portable, and easily lost or misplaced. Take steps to ensure that your data is protected.

Email and Instant Messaging (IM) – Email and IM messages hit numerous servers and routers, before reaching their final destination, and can be intercepted at any stage of this journey. If they are not encrypted, the data is vulnerable to being accessed. If your email contains sensitive data, consider encrypting it rather than sending it in clear text.

Personal Digital Assistants (PDAs) – These devices can hold large amounts of data. Because of their small size, they can be easily lost or stolen, which puts the data at risk.

Wireless networks – Confidential and valuable data can be intercepted by hackers while being transmitted over wireless networks, unless appropriate encryption is employed. In order to prevent unauthorized access, wireless networks need to be configured to turn encryption functionality on.

Backup tapes and media – Lost or stolen backup tapes, and other storage media, can cause data breach. These items should be encrypted to prevent unauthorized access.

Produced in part by US-CERT

Questions or comments?
E-mail us at eSecurity@state.de.us

Visit the Delaware Cyber Security website for more eSecurity Newsletters